

# nginx:stable (debian 12.11) - Trivy Report - 2025-09-01 22:43:18.858511192 +0100 +01 m=+0.128161645

					debian
Package	Vulnerability ID	Severity	Installed Version	Fixed Version	
apt	CVE-2011-3374	LOW	2.6.1		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugs.debian.org/cgi-bin/bugrep">https://bugs.debian.org/cgi-bin/bugrep</a> <a href="https://people.canonical.com/~ubuntu-">https://people.canonical.com/~ubuntu-</a> <a href="https://seclists.org/fulldisclosure/2011/">https://seclists.org/fulldisclosure/2011/</a>
bash	TEMP-0841856-B18BAF	LOW	5.2.15-2+b8		
bsdutils	CVE-2022-0563	LOW	1:2.38.1-5+deb12u3		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://blog.trailofbits.com/2023/02/16/">https://blog.trailofbits.com/2023/02/16/</a> <a href="https://lore.kernel.org/util-linux/202202">https://lore.kernel.org/util-linux/202202</a> <a href="https://lore.kernel.org/util-linux/202202">https://lore.kernel.org/util-linux/202202</a>
coreutils	CVE-2016-2781	LOW	9.1-1		<a href="http://seclists.org/oss-sec/2016/q1/452">http://seclists.org/oss-sec/2016/q1/452</a> <a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
coreutils	CVE-2017-18018	LOW	9.1-1		<a href="http://lists.gnu.org/archive/html/coreutil">http://lists.gnu.org/archive/html/coreutil</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://www.cve.org/CVERecord?id=C">https://www.cve.org/CVERecord?id=C</a>
coreutils	CVE-2025-5278	LOW	9.1-1		<a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
curl	CVE-2024-2379	LOW	7.88.1-10+deb12u12		<a href="http://seclists.org/fulldisclosure/2024/J">http://seclists.org/fulldisclosure/2024/J</a> <a href="http://seclists.org/fulldisclosure/2024/J">http://seclists.org/fulldisclosure/2024/J</a> <a href="http://seclists.org/fulldisclosure/2024/J">http://seclists.org/fulldisclosure/2024/J</a> <a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a>
curl	CVE-2025-0725	LOW	7.88.1-10+deb12u12		<a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
dpkg	CVE-2025-6297	UNKNOWN	1.21.22		<a href="https://git.dpkg.org/cgiit/dpkg/dpkg.git/c">https://git.dpkg.org/cgiit/dpkg/dpkg.git/c</a>
gcc-12-base	CVE-2022-27943	LOW	12.2.0-14+deb12u1		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://gcc.gnu.org/bugzilla/show_bug">https://gcc.gnu.org/bugzilla/show_bug</a> <a href="https://gcc.gnu.org/git/gitweb.cgi?p=gc">https://gcc.gnu.org/git/gitweb.cgi?p=gc</a> <a href="https://gcc.gnu.org/git/gitweb.cgi?p=gc">https://gcc.gnu.org/git/gitweb.cgi?p=gc</a>
gpgv	CVE-2022-3219	LOW	2.2.40-1.1		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/show_bug.c">https://bugzilla.redhat.com/show_bug.c</a> <a href="https://dev.gnupg.org/D556">https://dev.gnupg.org/D556</a> <a href="https://dev.gnupg.org/T5993">https://dev.gnupg.org/T5993</a>
gpgv	CVE-2025-30258	LOW	2.2.40-1.1		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://dev.gnupg.org/T7527">https://dev.gnupg.org/T7527</a> <a href="https://dev.gnupg.org/rG48978ccb4e2f">https://dev.gnupg.org/rG48978ccb4e2f</a> <a href="https://lists.gnupg.org/pipermail/gnupg">https://lists.gnupg.org/pipermail/gnupg</a>
libaom3	CVE-2023-6879	CRITICAL	3.6.0-1+deb12u1		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://aomedioa.googlesource.com/aor">https://aomedioa.googlesource.com/aor</a> <a href="https://crbug.com/aomedioa/3491">https://crbug.com/aomedioa/3491</a> <a href="https://lists.fedoraproject.org/archives/">https://lists.fedoraproject.org/archives/</a>
libaom3	CVE-2023-39616	HIGH	3.6.0-1+deb12u1		<a href="https://bugs.chromium.org/p/aomedioa/i">https://bugs.chromium.org/p/aomedioa/i</a>
libapt-pkg6.0	CVE-2011-3374	LOW	2.6.1		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugs.debian.org/cgi-bin/bugrep">https://bugs.debian.org/cgi-bin/bugrep</a> <a href="https://people.canonical.com/~ubuntu-">https://people.canonical.com/~ubuntu-</a> <a href="https://seclists.org/fulldisclosure/2011/">https://seclists.org/fulldisclosure/2011/</a>
libblkid1	CVE-2022-0563	LOW	2.38.1-5+deb12u3		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://blog.trailofbits.com/2023/02/16/">https://blog.trailofbits.com/2023/02/16/</a> <a href="https://lore.kernel.org/util-linux/202202">https://lore.kernel.org/util-linux/202202</a> <a href="https://lore.kernel.org/util-linux/202202">https://lore.kernel.org/util-linux/202202</a>
libc-bin	CVE-2025-4802	HIGH	2.36-9+deb12u10		<a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
libc-bin	CVE-2025-8058	MEDIUM	2.36-9+deb12u10		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2383146">https://bugzilla.redhat.com/2383146</a> <a href="https://errata.almalinux.org/10/ALSA-2">https://errata.almalinux.org/10/ALSA-2</a>

libc-bin	CVE-2010-4756	LOW	2.36-9+deb12u10	<a href="http://cxib.net/stuff/glob-0day.c">http://cxib.net/stuff/glob-0day.c</a> <a href="http://securityreason.com/achievement">http://securityreason.com/achievement</a> <a href="http://securityreason.com/exploitalert/9">http://securityreason.com/exploitalert/9</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
libc-bin	CVE-2018-20796	LOW	2.36-9+deb12u10	<a href="http://www.securityfocus.com/bid/1071">http://www.securityfocus.com/bid/1071</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://debbugs.gnu.org/cgi/bugreport.">https://debbugs.gnu.org/cgi/bugreport.</a> <a href="https://lists.gnu.org/archive/html/bug-g">https://lists.gnu.org/archive/html/bug-g</a>
libc-bin	CVE-2019-1010022	LOW	2.36-9+deb12u10	<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://security-tracker.debian.org/trac">https://security-tracker.debian.org/trac</a> <a href="https://sourceware.org/bugzilla/show_t">https://sourceware.org/bugzilla/show_t</a>
libc-bin	CVE-2019-1010023	LOW	2.36-9+deb12u10	<a href="http://www.securityfocus.com/bid/1091">http://www.securityfocus.com/bid/1091</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://security-tracker.debian.org/trac">https://security-tracker.debian.org/trac</a>
libc-bin	CVE-2019-1010024	LOW	2.36-9+deb12u10	<a href="http://www.securityfocus.com/bid/1091">http://www.securityfocus.com/bid/1091</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://security-tracker.debian.org/trac">https://security-tracker.debian.org/trac</a>
libc-bin	CVE-2019-1010025	LOW	2.36-9+deb12u10	<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://security-tracker.debian.org/trac">https://security-tracker.debian.org/trac</a> <a href="https://sourceware.org/bugzilla/show_t">https://sourceware.org/bugzilla/show_t</a>
libc-bin	CVE-2019-9192	LOW	2.36-9+deb12u10	<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://sourceware.org/bugzilla/show_t">https://sourceware.org/bugzilla/show_t</a> <a href="https://support.f5.com/csp/article/K263">https://support.f5.com/csp/article/K263</a>
libc6	CVE-2025-4802	HIGH	2.36-9+deb12u10	<a href="http://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-seci</a> <a href="http://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-seci</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
libc6	CVE-2025-8058	MEDIUM	2.36-9+deb12u10	<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2383146">https://bugzilla.redhat.com/2383146</a> <a href="https://errata.almalinux.org/10/ALSA-2">https://errata.almalinux.org/10/ALSA-2</a>
libc6	CVE-2010-4756	LOW	2.36-9+deb12u10	<a href="http://cxib.net/stuff/glob-0day.c">http://cxib.net/stuff/glob-0day.c</a> <a href="http://securityreason.com/achievement">http://securityreason.com/achievement</a> <a href="http://securityreason.com/exploitalert/9">http://securityreason.com/exploitalert/9</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
libc6	CVE-2018-20796	LOW	2.36-9+deb12u10	<a href="http://www.securityfocus.com/bid/1071">http://www.securityfocus.com/bid/1071</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://debbugs.gnu.org/cgi/bugreport.">https://debbugs.gnu.org/cgi/bugreport.</a> <a href="https://lists.gnu.org/archive/html/bug-g">https://lists.gnu.org/archive/html/bug-g</a>
libc6	CVE-2019-1010022	LOW	2.36-9+deb12u10	<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://security-tracker.debian.org/trac">https://security-tracker.debian.org/trac</a> <a href="https://sourceware.org/bugzilla/show_t">https://sourceware.org/bugzilla/show_t</a>
libc6	CVE-2019-1010023	LOW	2.36-9+deb12u10	<a href="http://www.securityfocus.com/bid/1091">http://www.securityfocus.com/bid/1091</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://security-tracker.debian.org/trac">https://security-tracker.debian.org/trac</a>
libc6	CVE-2019-1010024	LOW	2.36-9+deb12u10	<a href="http://www.securityfocus.com/bid/1091">http://www.securityfocus.com/bid/1091</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://security-tracker.debian.org/trac">https://security-tracker.debian.org/trac</a>
libc6	CVE-2019-1010025	LOW	2.36-9+deb12u10	<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://security-tracker.debian.org/trac">https://security-tracker.debian.org/trac</a> <a href="https://sourceware.org/bugzilla/show_t">https://sourceware.org/bugzilla/show_t</a>
libc6	CVE-2019-9192	LOW	2.36-9+deb12u10	<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://sourceware.org/bugzilla/show_t">https://sourceware.org/bugzilla/show_t</a> <a href="https://support.f5.com/csp/article/K263">https://support.f5.com/csp/article/K263</a>
libcurl4	CVE-2024-2379	LOW	7.88.1-10+deb12u12	<a href="http://seclists.org/fulldisclosure/2024/J">http://seclists.org/fulldisclosure/2024/J</a> <a href="http://seclists.org/fulldisclosure/2024/J">http://seclists.org/fulldisclosure/2024/J</a> <a href="http://seclists.org/fulldisclosure/2024/J">http://seclists.org/fulldisclosure/2024/J</a> <a href="http://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-seci</a>
libcurl4	CVE-2025-0725	LOW	7.88.1-10+deb12u12	<a href="http://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-seci</a> <a href="http://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-seci</a> <a href="http://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-seci</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
libdav1d6	CVE-2023-32570	MEDIUM	1.0.0-2+deb12u1	<a href="https://code.videolan.org/videolan/dav">https://code.videolan.org/videolan/dav</a> <a href="https://code.videolan.org/videolan/dav">https://code.videolan.org/videolan/dav</a> <a href="https://lists.fedoraproject.org/archives/">https://lists.fedoraproject.org/archives/</a> <a href="https://lists.fedoraproject.org/archives/">https://lists.fedoraproject.org/archives/</a>

libde265-0	CVE-2023-51792	MEDIUM	1.0.11-1+deb12u2		<a href="https://github.com/strukturag/libde265">https://github.com/strukturag/libde265</a> <a href="https://github.com/strukturag/libde265/">https://github.com/strukturag/libde265/</a> <a href="https://lists.fedoraproject.org/archives/">https://lists.fedoraproject.org/archives/</a> <a href="https://lists.fedoraproject.org/archives/">https://lists.fedoraproject.org/archives/</a>
libde265-0	CVE-2024-38949	MEDIUM	1.0.11-1+deb12u2		<a href="https://github.com/strukturag/libde265/">https://github.com/strukturag/libde265/</a> <a href="https://github.com/zhangteng0526/CVE">https://github.com/zhangteng0526/CVE</a> <a href="https://www.cve.org/CVERecord?id=C">https://www.cve.org/CVERecord?id=C</a>
libde265-0	CVE-2024-38950	MEDIUM	1.0.11-1+deb12u2		<a href="https://github.com/strukturag/libde265/">https://github.com/strukturag/libde265/</a> <a href="https://github.com/zhangteng0526/CVE">https://github.com/zhangteng0526/CVE</a> <a href="https://www.cve.org/CVERecord?id=C">https://www.cve.org/CVERecord?id=C</a>
libexpat1	CVE-2023-52425	HIGH	2.5.0-1+deb12u1		<a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2262877">https://bugzilla.redhat.com/2262877</a>
libexpat1	CVE-2024-8176	HIGH	2.5.0-1+deb12u1		<a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>
libexpat1	CVE-2024-50602	MEDIUM	2.5.0-1+deb12u1		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2321987">https://bugzilla.redhat.com/2321987</a> <a href="https://bugzilla.redhat.com/show_bug.c">https://bugzilla.redhat.com/show_bug.c</a>
libexpat1	CVE-2023-52426	LOW	2.5.0-1+deb12u1		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://cwe.mitre.org/data/definitions/7">https://cwe.mitre.org/data/definitions/7</a> <a href="https://github.com/libexpat/libexpat/cor">https://github.com/libexpat/libexpat/cor</a> <a href="https://github.com/libexpat/libexpat/pul">https://github.com/libexpat/libexpat/pul</a>
libexpat1	CVE-2024-28757	LOW	2.5.0-1+deb12u1		<a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2262877">https://bugzilla.redhat.com/2262877</a>
libgcc-s1	CVE-2022-27943	LOW	12.2.0-14+deb12u1		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://gcc.gnu.org/bugzilla/show_bug">https://gcc.gnu.org/bugzilla/show_bug</a> <a href="https://gcc.gnu.org/git/gitweb.cgi?p=gc">https://gcc.gnu.org/git/gitweb.cgi?p=gc</a> <a href="https://gcc.gnu.org/git/gitweb.cgi?p=gc">https://gcc.gnu.org/git/gitweb.cgi?p=gc</a>
libgcrypt20	CVE-2018-6829	LOW	1.10.1-3		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://github.com/weikengchen/attack">https://github.com/weikengchen/attack</a> <a href="https://github.com/weikengchen/attack">https://github.com/weikengchen/attack</a> <a href="https://lists.gnupg.org/pipermail/gcrypt">https://lists.gnupg.org/pipermail/gcrypt</a>
libgcrypt20	CVE-2024-2236	LOW	1.10.1-3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
libgnutls30	CVE-2011-3389	LOW	3.7.9-2+deb12u5		<a href="http://arcticdog.wordpress.com/2012/0">http://arcticdog.wordpress.com/2012/0</a> <a href="http://blog.mozilla.com/security/2011/0">http://blog.mozilla.com/security/2011/0</a> <a href="http://blogs.technet.com/b/msrc/archiv">http://blogs.technet.com/b/msrc/archiv</a> <a href="http://blogs.technet.com/b/srd/archive/">http://blogs.technet.com/b/srd/archive/</a>
libgssapi-krb5-2	CVE-2025-3576	MEDIUM	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>
libgssapi-krb5-2	CVE-2018-5709	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://github.com/poojamnit/Kerberos">https://github.com/poojamnit/Kerberos</a> <a href="https://lists.apache.org/thread.html/r9f">https://lists.apache.org/thread.html/r9f</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a>
libgssapi-krb5-2	CVE-2024-26458	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2266731">https://bugzilla.redhat.com/2266731</a> <a href="https://bugzilla.redhat.com/2266740">https://bugzilla.redhat.com/2266740</a>
libgssapi-krb5-2	CVE-2024-26461	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2266731">https://bugzilla.redhat.com/2266731</a> <a href="https://bugzilla.redhat.com/2266740">https://bugzilla.redhat.com/2266740</a>
libheif1	CVE-2023-49463	LOW	1.15.1-1+deb12u1		<a href="https://github.com/strukturag/libheif">https://github.com/strukturag/libheif</a> <a href="https://github.com/strukturag/libheif/iss">https://github.com/strukturag/libheif/iss</a> <a href="https://ubuntu.com/security/notices/US">https://ubuntu.com/security/notices/US</a> <a href="https://www.cve.org/CVERecord?id=C">https://www.cve.org/CVERecord?id=C</a>
libheif1	CVE-2024-25269	LOW	1.15.1-1+deb12u1		<a href="https://github.com/strukturag/libheif/iss">https://github.com/strukturag/libheif/iss</a>
libjbig0	CVE-2017-9937	LOW	2.1-6.1		<a href="http://bugzilla.maptools.org/show_bug">http://bugzilla.maptools.org/show_bug</a> <a href="http://www.securityfocus.com/bid/9930">http://www.securityfocus.com/bid/9930</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://lists.apache.org/thread.html/r9f">https://lists.apache.org/thread.html/r9f</a>
libk5crypto3	CVE-2025-3576	MEDIUM	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>

libk5crypto3	CVE-2018-5709	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://github.com/poojamnit/Kerberos">https://github.com/poojamnit/Kerberos</a> <a href="https://lists.apache.org/thread.html/rf9f">https://lists.apache.org/thread.html/rf9f</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a>
libk5crypto3	CVE-2024-26458	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2266731">https://bugzilla.redhat.com/2266731</a> <a href="https://bugzilla.redhat.com/2266740">https://bugzilla.redhat.com/2266740</a>
libk5crypto3	CVE-2024-26461	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2266731">https://bugzilla.redhat.com/2266731</a> <a href="https://bugzilla.redhat.com/2266740">https://bugzilla.redhat.com/2266740</a>
libkrb5-3	CVE-2025-3576	MEDIUM	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>
libkrb5-3	CVE-2018-5709	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://github.com/poojamnit/Kerberos">https://github.com/poojamnit/Kerberos</a> <a href="https://lists.apache.org/thread.html/rf9f">https://lists.apache.org/thread.html/rf9f</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a>
libkrb5-3	CVE-2024-26458	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2266731">https://bugzilla.redhat.com/2266731</a> <a href="https://bugzilla.redhat.com/2266740">https://bugzilla.redhat.com/2266740</a>
libkrb5-3	CVE-2024-26461	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2266731">https://bugzilla.redhat.com/2266731</a> <a href="https://bugzilla.redhat.com/2266740">https://bugzilla.redhat.com/2266740</a>
libkrb5support0	CVE-2025-3576	MEDIUM	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>
libkrb5support0	CVE-2018-5709	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://github.com/poojamnit/Kerberos">https://github.com/poojamnit/Kerberos</a> <a href="https://lists.apache.org/thread.html/rf9f">https://lists.apache.org/thread.html/rf9f</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a>
libkrb5support0	CVE-2024-26458	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2266731">https://bugzilla.redhat.com/2266731</a> <a href="https://bugzilla.redhat.com/2266740">https://bugzilla.redhat.com/2266740</a>
libkrb5support0	CVE-2024-26461	LOW	1.20.1-2+deb12u3		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://bugzilla.redhat.com/2266731">https://bugzilla.redhat.com/2266731</a> <a href="https://bugzilla.redhat.com/2266740">https://bugzilla.redhat.com/2266740</a>
libldap-2.5-0	CVE-2023-2953	HIGH	2.5.13+dfsg-5		<a href="http://seclists.org/fulldisclosure/2023/J">http://seclists.org/fulldisclosure/2023/J</a> <a href="http://seclists.org/fulldisclosure/2023/J">http://seclists.org/fulldisclosure/2023/J</a> <a href="http://seclists.org/fulldisclosure/2023/J">http://seclists.org/fulldisclosure/2023/J</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>
libldap-2.5-0	CVE-2015-3276	LOW	2.5.13+dfsg-5		<a href="http://rhn.redhat.com/errata/RHSA-201">http://rhn.redhat.com/errata/RHSA-201</a> <a href="http://www.oracle.com/technetwork/top">http://www.oracle.com/technetwork/top</a> <a href="http://www.securitytracker.com/id/1034">http://www.securitytracker.com/id/1034</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
libldap-2.5-0	CVE-2017-14159	LOW	2.5.13+dfsg-5		<a href="http://www.openldap.org/its/index.cgi/?">http://www.openldap.org/its/index.cgi/?</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-20">https://nvd.nist.gov/vuln/detail/CVE-20</a> <a href="https://www.cve.org/CVERecord?id=C">https://www.cve.org/CVERecord?id=C</a>
libldap-2.5-0	CVE-2017-17740	LOW	2.5.13+dfsg-5		<a href="http://lists.opensuse.org/opensuse-sec">http://lists.opensuse.org/opensuse-sec</a> <a href="http://lists.opensuse.org/opensuse-sec">http://lists.opensuse.org/opensuse-sec</a> <a href="http://www.openldap.org/its/index.cgi/?">http://www.openldap.org/its/index.cgi/?</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
libldap-2.5-0	CVE-2020-15719	LOW	2.5.13+dfsg-5		<a href="http://lists.opensuse.org/opensuse-sec">http://lists.opensuse.org/opensuse-sec</a> <a href="http://lists.opensuse.org/opensuse-sec">http://lists.opensuse.org/opensuse-sec</a> <a href="https://access.redhat.com/errata/RHB/">https://access.redhat.com/errata/RHB/</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a>
libmount1	CVE-2022-0563	LOW	2.38.1-5+deb12u3		<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://blog.trailofbits.com/2023/02/16/">https://blog.trailofbits.com/2023/02/16/</a> <a href="https://lore.kernel.org/util-linux/202202">https://lore.kernel.org/util-linux/202202</a> <a href="https://lore.kernel.org/util-linux/202202">https://lore.kernel.org/util-linux/202202</a>
libpam-modules	CVE-2025-6020	HIGH	1.5.2-6+deb12u1		<a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>

libpam-modules	CVE-2024-10041	MEDIUM	1.5.2-6+deb12u1		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a>
libpam-modules	CVE-2024-22365	MEDIUM	1.5.2-6+deb12u1		<a href="http://www.openwall.com/lists/oss-sec/">http://www.openwall.com/lists/oss-sec/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a> <a href="https://bugzilla.redhat.com/2257722">https://bugzilla.redhat.com/2257722</a>
libpam-modules-bin	CVE-2025-6020	HIGH	1.5.2-6+deb12u1		<a href="http://www.openwall.com/lists/oss-sec/">http://www.openwall.com/lists/oss-sec/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>
libpam-modules-bin	CVE-2024-10041	MEDIUM	1.5.2-6+deb12u1		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a>
libpam-modules-bin	CVE-2024-22365	MEDIUM	1.5.2-6+deb12u1		<a href="http://www.openwall.com/lists/oss-sec/">http://www.openwall.com/lists/oss-sec/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a> <a href="https://bugzilla.redhat.com/2257722">https://bugzilla.redhat.com/2257722</a>
libpam-runtime	CVE-2025-6020	HIGH	1.5.2-6+deb12u1		<a href="http://www.openwall.com/lists/oss-sec/">http://www.openwall.com/lists/oss-sec/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>
libpam-runtime	CVE-2024-10041	MEDIUM	1.5.2-6+deb12u1		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a>
libpam-runtime	CVE-2024-22365	MEDIUM	1.5.2-6+deb12u1		<a href="http://www.openwall.com/lists/oss-sec/">http://www.openwall.com/lists/oss-sec/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a> <a href="https://bugzilla.redhat.com/2257722">https://bugzilla.redhat.com/2257722</a>
libpam0g	CVE-2025-6020	HIGH	1.5.2-6+deb12u1		<a href="http://www.openwall.com/lists/oss-sec/">http://www.openwall.com/lists/oss-sec/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a>
libpam0g	CVE-2024-10041	MEDIUM	1.5.2-6+deb12u1		<a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a>
libpam0g	CVE-2024-22365	MEDIUM	1.5.2-6+deb12u1		<a href="http://www.openwall.com/lists/oss-sec/">http://www.openwall.com/lists/oss-sec/</a> <a href="https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/</a> <a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a> <a href="https://bugzilla.redhat.com/2257722">https://bugzilla.redhat.com/2257722</a>
libpng16-16	CVE-2021-4214	LOW	1.6.39-2		<a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a> <a href="https://bugzilla.redhat.com/show_bug.cgi?id=202202">https://bugzilla.redhat.com/show_bug.cgi?id=202202</a> <a href="https://github.com/glennrp/libpng/issue/202202">https://github.com/glennrp/libpng/issue/202202</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2022-0202">https://nvd.nist.gov/vuln/detail/CVE-2022-0202</a>
libsmartcols1	CVE-2022-0563	LOW	2.38.1-5+deb12u3		<a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a> <a href="https://blog.trailofbits.com/2023/02/16/lorem-kernel-202202/">https://blog.trailofbits.com/2023/02/16/lorem-kernel-202202/</a> <a href="https://lore.kernel.org/util-linux/20220202">https://lore.kernel.org/util-linux/20220202</a> <a href="https://lore.kernel.org/util-linux/20220202">https://lore.kernel.org/util-linux/20220202</a>
libssl3	CVE-2025-27587	LOW	3.0.17-1~deb12u2		<a href="https://github.com/openssl/openssl/issues/19954">https://github.com/openssl/openssl/issues/19954</a> <a href="https://minerva.crocs.fi.muni.cz/~mimoz/2025-02-27-openssl-cve-2025-27587/">https://minerva.crocs.fi.muni.cz/~mimoz/2025-02-27-openssl-cve-2025-27587/</a> <a href="https://www.cve.org/CVERecord?id=CVE-2025-27587">https://www.cve.org/CVERecord?id=CVE-2025-27587</a>
libstdc++6	CVE-2022-27943	LOW	12.2.0-14+deb12u1		<a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a> <a href="https://gcc.gnu.org/bugzilla/show_bug.cgi?id=108881">https://gcc.gnu.org/bugzilla/show_bug.cgi?id=108881</a> <a href="https://gcc.gnu.org/git/gitweb.cgi?p=gcc/gcc.git;a=commit;h=7a1b1b1">https://gcc.gnu.org/git/gitweb.cgi?p=gcc/gcc.git;a=commit;h=7a1b1b1</a> <a href="https://gcc.gnu.org/git/gitweb.cgi?p=gcc/gcc.git;a=commit;h=7a1b1b1">https://gcc.gnu.org/git/gitweb.cgi?p=gcc/gcc.git;a=commit;h=7a1b1b1</a>
libsystemd0	CVE-2013-4392	LOW	252.38-1~deb12u1		<a href="http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=744444">http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=744444</a> <a href="http://www.openwall.com/lists/oss-sec/">http://www.openwall.com/lists/oss-sec/</a> <a href="https://access.redhat.com/security/cve/">https://access.redhat.com/security/cve/</a> <a href="https://bugzilla.redhat.com/show_bug.cgi?id=108881">https://bugzilla.redhat.com/show_bug.cgi?id=108881</a>
libsystemd0	CVE-2023-31437	LOW	252.38-1~deb12u1		<a href="https://github.com/kastel-security/Journald-2023-02-28">https://github.com/kastel-security/Journald-2023-02-28</a> <a href="https://github.com/kastel-security/Journald-2023-02-28">https://github.com/kastel-security/Journald-2023-02-28</a> <a href="https://github.com/systemd/systemd/pull/25238">https://github.com/systemd/systemd/pull/25238</a>
libsystemd0	CVE-2023-31438	LOW	252.38-1~deb12u1		<a href="https://github.com/kastel-security/Journald-2023-02-28">https://github.com/kastel-security/Journald-2023-02-28</a> <a href="https://github.com/kastel-security/Journald-2023-02-28">https://github.com/kastel-security/Journald-2023-02-28</a> <a href="https://github.com/systemd/systemd/pull/25238">https://github.com/systemd/systemd/pull/25238</a> <a href="https://github.com/systemd/systemd/pull/25238">https://github.com/systemd/systemd/pull/25238</a>
libsystemd0	CVE-2023-31439	LOW	252.38-1~deb12u1		<a href="https://github.com/kastel-security/Journald-2023-02-28">https://github.com/kastel-security/Journald-2023-02-28</a> <a href="https://github.com/kastel-security/Journald-2023-02-28">https://github.com/kastel-security/Journald-2023-02-28</a> <a href="https://github.com/systemd/systemd/pull/25238">https://github.com/systemd/systemd/pull/25238</a> <a href="https://github.com/systemd/systemd/pull/25238">https://github.com/systemd/systemd/pull/25238</a>



libtiff6	CVE-2023-52355	HIGH	4.5.0-6+deb12u2		<a href="https://access.redhat.com/security/cve/https://bugzilla.redhat.com/show_bug.cgi?id=2215865">https://access.redhat.com/security/cve/https://bugzilla.redhat.com/show_bug.cgi?id=2215865</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/62">https://gitlab.com/libtiff/libtiff/-/issues/62</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2023-52355">https://nvd.nist.gov/vuln/detail/CVE-2023-52355</a>
libtiff6	CVE-2023-6277	MEDIUM	4.5.0-6+deb12u2		<a href="http://seclists.org/fulldisclosure/2024/Jun/1">http://seclists.org/fulldisclosure/2024/Jun/1</a> <a href="http://seclists.org/fulldisclosure/2024/Jun/1">http://seclists.org/fulldisclosure/2024/Jun/1</a> <a href="http://seclists.org/fulldisclosure/2024/Jun/1">http://seclists.org/fulldisclosure/2024/Jun/1</a>
libtiff6	CVE-2017-16232	LOW	4.5.0-6+deb12u2		<a href="http://lists.opensuse.org/opensuse-security/2017/09/01/opensuse-security-announce-2017-09-01-1.html">http://lists.opensuse.org/opensuse-security/2017/09/01/opensuse-security-announce-2017-09-01-1.html</a> <a href="http://lists.opensuse.org/opensuse-security/2017/09/01/opensuse-security-announce-2017-09-01-1.html">http://lists.opensuse.org/opensuse-security/2017/09/01/opensuse-security-announce-2017-09-01-1.html</a> <a href="http://packetsfromsecurity.com/files/15">http://packetsfromsecurity.com/files/15</a> <a href="http://seclists.org/fulldisclosure/2018/D">http://seclists.org/fulldisclosure/2018/D</a>
libtiff6	CVE-2017-17973	LOW	4.5.0-6+deb12u2		<a href="http://bugzilla.maptools.org/show_bug.cgi?id=1023">http://bugzilla.maptools.org/show_bug.cgi?id=1023</a> <a href="http://www.securityfocus.com/bid/1023">http://www.securityfocus.com/bid/1023</a> <a href="https://access.redhat.com/security/cve/https://bugzilla.novell.com/show_bug.cgi?id=1023">https://access.redhat.com/security/cve/https://bugzilla.novell.com/show_bug.cgi?id=1023</a>
libtiff6	CVE-2017-5563	LOW	4.5.0-6+deb12u2		<a href="http://bugzilla.maptools.org/show_bug.cgi?id=9570">http://bugzilla.maptools.org/show_bug.cgi?id=9570</a> <a href="http://www.securityfocus.com/bid/9570">http://www.securityfocus.com/bid/9570</a> <a href="https://access.redhat.com/security/cve/https://nvd.nist.gov/vuln/detail/CVE-2017-5563">https://access.redhat.com/security/cve/https://nvd.nist.gov/vuln/detail/CVE-2017-5563</a>
libtiff6	CVE-2017-9117	LOW	4.5.0-6+deb12u2		<a href="http://bugzilla.maptools.org/show_bug.cgi?id=9858">http://bugzilla.maptools.org/show_bug.cgi?id=9858</a> <a href="http://www.securityfocus.com/bid/9858">http://www.securityfocus.com/bid/9858</a> <a href="https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/issues/85">https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/issues/85</a>
libtiff6	CVE-2018-10126	LOW	4.5.0-6+deb12u2		<a href="http://bugzilla.maptools.org/show_bug.cgi?id=1023">http://bugzilla.maptools.org/show_bug.cgi?id=1023</a> <a href="https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/issues/12">https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/issues/12</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/12">https://gitlab.com/libtiff/libtiff/-/issues/12</a> <a href="https://lists.apache.org/thread.html/rf9f">https://lists.apache.org/thread.html/rf9f</a>
libtiff6	CVE-2022-1210	LOW	4.5.0-6+deb12u2		<a href="https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/issues/46">https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/issues/46</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/46">https://gitlab.com/libtiff/libtiff/-/issues/46</a> <a href="https://gitlab.com/libtiff/libtiff/uploads/cve-2022-1210">https://gitlab.com/libtiff/libtiff/uploads/cve-2022-1210</a> <a href="https://nvd.nist.gov/vuln/detail/CVE-2022-1210">https://nvd.nist.gov/vuln/detail/CVE-2022-1210</a>
libtiff6	CVE-2023-1916	LOW	4.5.0-6+deb12u2		<a href="https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/issues/53">https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/issues/53</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/53">https://gitlab.com/libtiff/libtiff/-/issues/53</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/53">https://gitlab.com/libtiff/libtiff/-/issues/53</a>
libtiff6	CVE-2023-3164	LOW	4.5.0-6+deb12u2		<a href="https://access.redhat.com/security/cve/https://bugzilla.redhat.com/show_bug.cgi?id=2215865">https://access.redhat.com/security/cve/https://bugzilla.redhat.com/show_bug.cgi?id=2215865</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/54">https://gitlab.com/libtiff/libtiff/-/issues/54</a> <a href="https://gitlab.com/libtiff/libtiff/-/merge_requests/1">https://gitlab.com/libtiff/libtiff/-/merge_requests/1</a>
libtiff6	CVE-2023-6228	LOW	4.5.0-6+deb12u2		<a href="https://access.redhat.com/errata/RHSA-2023-0665">https://access.redhat.com/errata/RHSA-2023-0665</a> <a href="https://access.redhat.com/errata/RHSA-2023-0665">https://access.redhat.com/errata/RHSA-2023-0665</a> <a href="https://access.redhat.com/security/cve/https://bugzilla.redhat.com/2215865">https://access.redhat.com/security/cve/https://bugzilla.redhat.com/2215865</a>
libtiff6	CVE-2024-13978	LOW	4.5.0-6+deb12u2		<a href="http://www.libtiff.org/">http://www.libtiff.org/</a> <a href="https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/commit/2">https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/commit/2</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/64">https://gitlab.com/libtiff/libtiff/-/issues/64</a>
libtiff6	CVE-2025-8176	LOW	4.5.0-6+deb12u2		<a href="http://www.libtiff.org/">http://www.libtiff.org/</a> <a href="https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/commit/f">https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/commit/f</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/70">https://gitlab.com/libtiff/libtiff/-/issues/70</a>
libtiff6	CVE-2025-8177	LOW	4.5.0-6+deb12u2		<a href="http://www.libtiff.org/">http://www.libtiff.org/</a> <a href="https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/commit/e">https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/commit/e</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/71">https://gitlab.com/libtiff/libtiff/-/issues/71</a>
libtiff6	CVE-2025-8534	LOW	4.5.0-6+deb12u2		<a href="http://www.libtiff.org/">http://www.libtiff.org/</a> <a href="https://access.redhat.com/security/cve/https://drive.google.com/file/d/15JPA3t">https://access.redhat.com/security/cve/https://drive.google.com/file/d/15JPA3t</a> <a href="https://gitlab.com/libtiff/libtiff/-/commit/6">https://gitlab.com/libtiff/libtiff/-/commit/6</a>
libtiff6	CVE-2025-8851	LOW	4.5.0-6+deb12u2		<a href="http://www.libtiff.org/">http://www.libtiff.org/</a> <a href="https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/commit/8">https://access.redhat.com/security/cve/https://gitlab.com/libtiff/libtiff/-/commit/8</a> <a href="https://gitlab.com/libtiff/libtiff/-/commit/8">https://gitlab.com/libtiff/libtiff/-/commit/8</a>
libtiff6	CVE-2025-8961	LOW	4.5.0-6+deb12u2		<a href="http://www.libtiff.org/">http://www.libtiff.org/</a> <a href="https://access.redhat.com/security/cve/https://drive.google.com/file/d/15L4q2e">https://access.redhat.com/security/cve/https://drive.google.com/file/d/15L4q2e</a> <a href="https://gitlab.com/libtiff/libtiff/-/issues/72">https://gitlab.com/libtiff/libtiff/-/issues/72</a>
libtiff6	CVE-2025-9165	LOW	4.5.0-6+deb12u2		<a href="http://www.libtiff.org/">http://www.libtiff.org/</a> <a href="https://access.redhat.com/security/cve/https://drive.google.com/file/d/1FWHm">https://access.redhat.com/security/cve/https://drive.google.com/file/d/1FWHm</a> <a href="https://gitlab.com/libtiff/libtiff/-/commit/e">https://gitlab.com/libtiff/libtiff/-/commit/e</a>

libtinfo6	CVE-2023-50495	MEDIUM	6.4-4		<a href="https://access.redhat.com/security/cve/https://lists.fedoraproject.org/archives/">https://access.redhat.com/security/cve/https://lists.fedoraproject.org/archives/</a> <a href="https://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n">https://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n</a>
libtinfo6	CVE-2025-6141	LOW	6.4-4		<a href="https://access.redhat.com/security/cvehttps://invisible-island.net/ncurses/NEVhttps://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n">https://access.redhat.com/security/cvehttps://invisible-island.net/ncurses/NEVhttps://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n</a>
libudev1	CVE-2013-4392	LOW	252.38-1~deb12u1		<a href="http://bugs.debian.org/cgi-bin/bugreporhttp://www.openwall.com/lists/oss-secthttps://access.redhat.com/security/cvehttps://bugzilla.redhat.com/show_bug.c">http://bugs.debian.org/cgi-bin/bugreporhttp://www.openwall.com/lists/oss-secthttps://access.redhat.com/security/cvehttps://bugzilla.redhat.com/show_bug.c</a>
libudev1	CVE-2023-31437	LOW	252.38-1~deb12u1		<a href="https://github.com/kastel-security/Journhttps://github.com/kastel-security/Journhttps://github.com/systemd/systemd/rehttps://github.com/systemd/systemd/re">https://github.com/kastel-security/Journhttps://github.com/kastel-security/Journhttps://github.com/systemd/systemd/rehttps://github.com/systemd/systemd/re</a>
libudev1	CVE-2023-31438	LOW	252.38-1~deb12u1		<a href="https://github.com/kastel-security/Journhttps://github.com/kastel-security/Journhttps://github.com/systemd/systemd/phttps://github.com/systemd/systemd/re">https://github.com/kastel-security/Journhttps://github.com/kastel-security/Journhttps://github.com/systemd/systemd/phttps://github.com/systemd/systemd/re</a>
libudev1	CVE-2023-31439	LOW	252.38-1~deb12u1		<a href="https://github.com/kastel-security/Journhttps://github.com/kastel-security/Journhttps://github.com/systemd/systemd/phttps://github.com/systemd/systemd/rehttps://github.com/systemd/systemd/re">https://github.com/kastel-security/Journhttps://github.com/kastel-security/Journhttps://github.com/systemd/systemd/phttps://github.com/systemd/systemd/rehttps://github.com/systemd/systemd/re</a>
libuuid1	CVE-2022-0563	LOW	2.38.1-5+deb12u3		<a href="https://access.redhat.com/security/cvehttps://blog.trailofbits.com/2023/02/16:/https://lore.kernel.org/util-linux/202202https://lore.kernel.org/util-linux/202202">https://access.redhat.com/security/cvehttps://blog.trailofbits.com/2023/02/16:/https://lore.kernel.org/util-linux/202202https://lore.kernel.org/util-linux/202202</a>
libxml2	CVE-2025-49794	CRITICAL	2.9.14+dfsg-1.3~deb12u2		<a href="https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/</a>
libxml2	CVE-2025-49796	CRITICAL	2.9.14+dfsg-1.3~deb12u2		<a href="https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/</a>
libxml2	CVE-2025-6021	HIGH	2.9.14+dfsg-1.3~deb12u2		<a href="https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/</a>
libxml2	CVE-2025-6170	LOW	2.9.14+dfsg-1.3~deb12u2		<a href="https://access.redhat.com/security/cvehttps://bugzilla.redhat.com/show_bug.chttps://gitlab.gnome.org/GNOME/libxmhttps://nvd.nist.gov/vuln/detail/CVE-20;">https://access.redhat.com/security/cvehttps://bugzilla.redhat.com/show_bug.chttps://gitlab.gnome.org/GNOME/libxmhttps://nvd.nist.gov/vuln/detail/CVE-20;</a>
libxml2	CVE-2025-8732	LOW	2.9.14+dfsg-1.3~deb12u2		<a href="https://access.redhat.com/security/cvehttps://drive.google.com/file/d/1woleYVhttps://gitlab.gnome.org/GNOME/libxmhttps://gitlab.gnome.org/GNOME/libxm">https://access.redhat.com/security/cvehttps://drive.google.com/file/d/1woleYVhttps://gitlab.gnome.org/GNOME/libxmhttps://gitlab.gnome.org/GNOME/libxm</a>
libxml2	DSA-5990-1	UNKNOWN	2.9.14+dfsg-1.3~deb12u2	2.9.14+dfsg-1.3~deb12u4	
libxslt1.1	CVE-2025-7424	HIGH	1.1.35-1+deb12u1	1.1.35-1+deb12u2	<a href="https://access.redhat.com/security/cvehttps://bugzilla.redhat.com/show_bug.chttps://nvd.nist.gov/vuln/detail/CVE-20;https://www.cve.org/CVERecord?id=C">https://access.redhat.com/security/cvehttps://bugzilla.redhat.com/show_bug.chttps://nvd.nist.gov/vuln/detail/CVE-20;https://www.cve.org/CVERecord?id=C</a>
libxslt1.1	CVE-2025-7425	HIGH	1.1.35-1+deb12u1		<a href="https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/">https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/https://access.redhat.com/errata/RHS/</a>
libxslt1.1	CVE-2023-40403	MEDIUM	1.1.35-1+deb12u1	1.1.35-1+deb12u2	<a href="http://seclists.org/fulldisclosure/2023/Ohttp://seclists.org/fulldisclosure/2023/Ohttp://seclists.org/fulldisclosure/2023/Ohttp://seclists.org/fulldisclosure/2023/O">http://seclists.org/fulldisclosure/2023/Ohttp://seclists.org/fulldisclosure/2023/Ohttp://seclists.org/fulldisclosure/2023/Ohttp://seclists.org/fulldisclosure/2023/O</a>
libxslt1.1	CVE-2015-9019	LOW	1.1.35-1+deb12u1		<a href="https://access.redhat.com/security/cvehttps://bugzilla.gnome.org/show_bug.chhttps://bugzilla.suse.com/show_bug.cghttps://nvd.nist.gov/vuln/detail/CVE-20;">https://access.redhat.com/security/cvehttps://bugzilla.gnome.org/show_bug.chhttps://bugzilla.suse.com/show_bug.cghttps://nvd.nist.gov/vuln/detail/CVE-20;</a>
login	CVE-2007-5686	LOW	1:4.13+dfsg1-1+deb12u1		<a href="http://secunia.com/advisories/27215http://www.securityfocus.com/archive/1http://www.securityfocus.com/archive/1http://www.securityfocus.com/bid/2604">http://secunia.com/advisories/27215http://www.securityfocus.com/archive/1http://www.securityfocus.com/archive/1http://www.securityfocus.com/bid/2604</a>
login	CVE-2024-56433	LOW	1:4.13+dfsg1-1+deb12u1		<a href="https://access.redhat.com/security/cvehttps://github.com/shadow-maint/shadhttps://github.com/shadow-maint/shadhttps://github.com/shadow-maint/shadhttps://github.com/shadow-maint/shad">https://access.redhat.com/security/cvehttps://github.com/shadow-maint/shadhttps://github.com/shadow-maint/shadhttps://github.com/shadow-maint/shad</a>
login	TEMP-0628843-DBAD28	LOW	1:4.13+dfsg1-1+deb12u1		

mount	CVE-2022-0563	LOW	2.38.1-5+deb12u3		<a href="https://access.redhat.com/security/cve/https://blog.trailofbits.com/2023/02/16/https://lore.kernel.org/util-linux/202202https://lore.kernel.org/util-linux/202202">https://access.redhat.com/security/cve/https://blog.trailofbits.com/2023/02/16/https://lore.kernel.org/util-linux/202202https://lore.kernel.org/util-linux/202202</a>
ncurses-base	CVE-2023-50495	MEDIUM	6.4-4		<a href="https://access.redhat.com/security/cve/https://lists.fedoraproject.org/archives/https://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n">https://access.redhat.com/security/cve/https://lists.fedoraproject.org/archives/https://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n</a>
ncurses-base	CVE-2025-6141	LOW	6.4-4		<a href="https://access.redhat.com/security/cve/https://invisible-island.net/ncurses/NEVhttps://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n">https://access.redhat.com/security/cve/https://invisible-island.net/ncurses/NEVhttps://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n</a>
ncurses-bin	CVE-2023-50495	MEDIUM	6.4-4		<a href="https://access.redhat.com/security/cve/https://lists.fedoraproject.org/archives/https://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n">https://access.redhat.com/security/cve/https://lists.fedoraproject.org/archives/https://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n</a>
ncurses-bin	CVE-2025-6141	LOW	6.4-4		<a href="https://access.redhat.com/security/cve/https://invisible-island.net/ncurses/NEVhttps://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n">https://access.redhat.com/security/cve/https://invisible-island.net/ncurses/NEVhttps://lists.gnu.org/archive/html/bug-nhttps://lists.gnu.org/archive/html/bug-n</a>
nginx	CVE-2009-4487	LOW	1.28.0-1~bookworm		<a href="http://www.securityfocus.com/archive/1http://www.securityfocus.com/bid/3771http://www.ush.it/team/ush/hack_httpdhttps://access.redhat.com/security/cve">http://www.securityfocus.com/archive/1http://www.securityfocus.com/bid/3771http://www.ush.it/team/ush/hack_httpdhttps://access.redhat.com/security/cve</a>
nginx	CVE-2013-0337	LOW	1.28.0-1~bookworm		<a href="http://secunia.com/advisories/55181http://security.gentoo.org/glsa/glsa-201http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci">http://secunia.com/advisories/55181http://security.gentoo.org/glsa/glsa-201http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci</a>
nginx	CVE-2023-44487	LOW	1.28.0-1~bookworm		<a href="http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci</a>
nginx	CVE-2025-53859	LOW	1.28.0-1~bookworm		<a href="https://access.redhat.com/security/cve/https://my.f5.com/manage/s/article/K0https://nginx.org/download/patch.2025https://nvd.nist.gov/vuln/detail/CVE-20">https://access.redhat.com/security/cve/https://my.f5.com/manage/s/article/K0https://nginx.org/download/patch.2025https://nvd.nist.gov/vuln/detail/CVE-20</a>
openssl	CVE-2025-27587	LOW	3.0.17-1~deb12u2		<a href="https://github.com/openssl/openssl/isshttps://minerva.crocs.fi.muni.czhttps://www.cve.org/CVERecord?id=C">https://github.com/openssl/openssl/isshttps://minerva.crocs.fi.muni.czhttps://www.cve.org/CVERecord?id=C</a>
passwd	CVE-2007-5686	LOW	1:4.13+dfsg1-1+deb12u1		<a href="http://secunia.com/advisories/27215http://www.securityfocus.com/archive/1http://www.securityfocus.com/archive/1http://www.securityfocus.com/bid/2604">http://secunia.com/advisories/27215http://www.securityfocus.com/archive/1http://www.securityfocus.com/archive/1http://www.securityfocus.com/bid/2604</a>
passwd	CVE-2024-56433	LOW	1:4.13+dfsg1-1+deb12u1		<a href="https://access.redhat.com/security/cve/https://github.com/shadow-maint/shadhttps://github.com/shadow-maint/shadhttps://github.com/shadow-maint/shad">https://access.redhat.com/security/cve/https://github.com/shadow-maint/shadhttps://github.com/shadow-maint/shadhttps://github.com/shadow-maint/shad</a>
passwd	TEMP-0628843-DBAD28	LOW	1:4.13+dfsg1-1+deb12u1		
perl-base	CVE-2023-31484	HIGH	5.36.0-7+deb12u2		<a href="http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci</a>
perl-base	CVE-2025-40909	MEDIUM	5.36.0-7+deb12u2		<a href="http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci</a>
perl-base	CVE-2011-4116	LOW	5.36.0-7+deb12u2		<a href="http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttps://access.redhat.com/security/cvehttps://github.com/Perl-Toolchain-Gang">http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttps://access.redhat.com/security/cvehttps://github.com/Perl-Toolchain-Gang</a>
perl-base	CVE-2023-31486	LOW	5.36.0-7+deb12u2		<a href="http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci">http://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-secihttp://www.openwall.com/lists/oss-seci</a>
sysvinit-utils	TEMP-0517018-A83CE6	LOW	3.06-4		
tar	CVE-2005-2541	LOW	1.34+dfsg-1.2+deb12u1		<a href="http://marc.info/?l=bugtraq&amp;m=112327https://access.redhat.com/security/cvehttps://lists.apache.org/thread.html/rc7https://nvd.nist.gov/vuln/detail/CVE-20">http://marc.info/?l=bugtraq&amp;m=112327https://access.redhat.com/security/cvehttps://lists.apache.org/thread.html/rc7https://nvd.nist.gov/vuln/detail/CVE-20</a>
tar	TEMP-0290435-0B57B5	LOW	1.34+dfsg-1.2+deb12u1		
util-linux	CVE-2022-0563	LOW	2.38.1-5+deb12u3		<a href="https://access.redhat.com/security/cve/https://blog.trailofbits.com/2023/02/16/https://lore.kernel.org/util-linux/202202https://lore.kernel.org/util-linux/202202">https://access.redhat.com/security/cve/https://blog.trailofbits.com/2023/02/16/https://lore.kernel.org/util-linux/202202https://lore.kernel.org/util-linux/202202</a>



util-linux-extra	CVE-2022-0563	LOW	2.38.1-5+deb12u3	<a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://blog.trailofbits.com/2023/02/16/">https://blog.trailofbits.com/2023/02/16/</a> <a href="https://lore.kernel.org/util-linux/202202">https://lore.kernel.org/util-linux/202202</a> <a href="https://lore.kernel.org/util-linux/202202">https://lore.kernel.org/util-linux/202202</a>
zlib1g	CVE-2023-45853	CRITICAL	1:1.2.13.dfsg-1	<a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="http://www.openwall.com/lists/oss-sec">http://www.openwall.com/lists/oss-sec</a> <a href="https://access.redhat.com/security/cve">https://access.redhat.com/security/cve</a> <a href="https://chromium.googlesource.com/ch">https://chromium.googlesource.com/ch</a>
No Misconfigurations found				